HiDDeN

Hiding Data With Deep Networks

HiDDeN Overview

HiDDeN is a deep learning framework that used in hiding information with image.2 main applications of this framework are steganography and digital watermarking. While steganography aims for the capacity and secrecy of the message, digital watermarking is focused on the decode’s robustness since watermarking is used to identify ownership of the image.

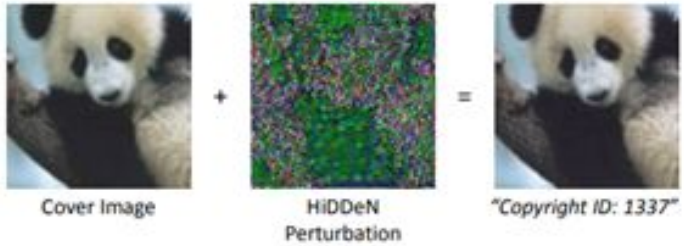
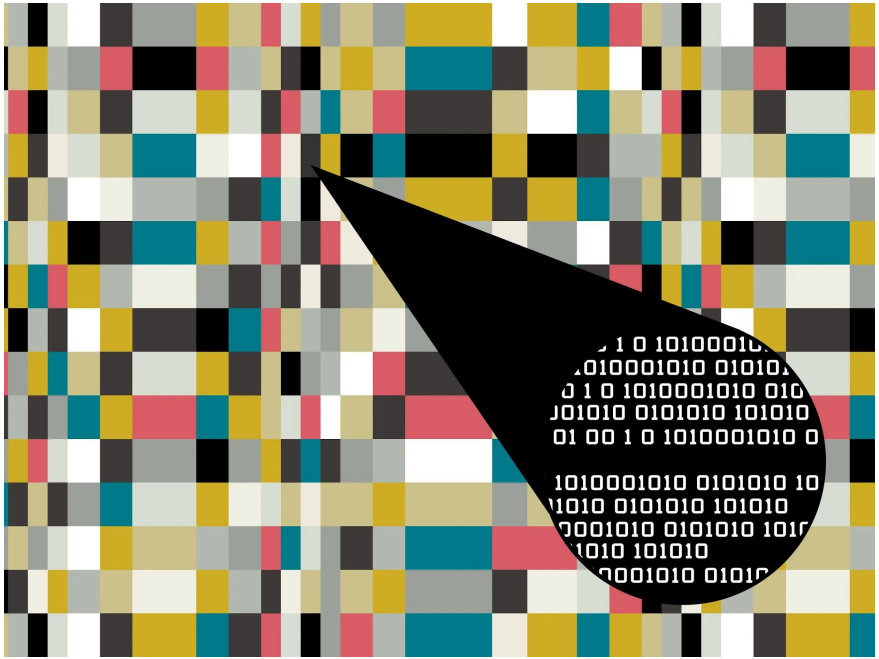
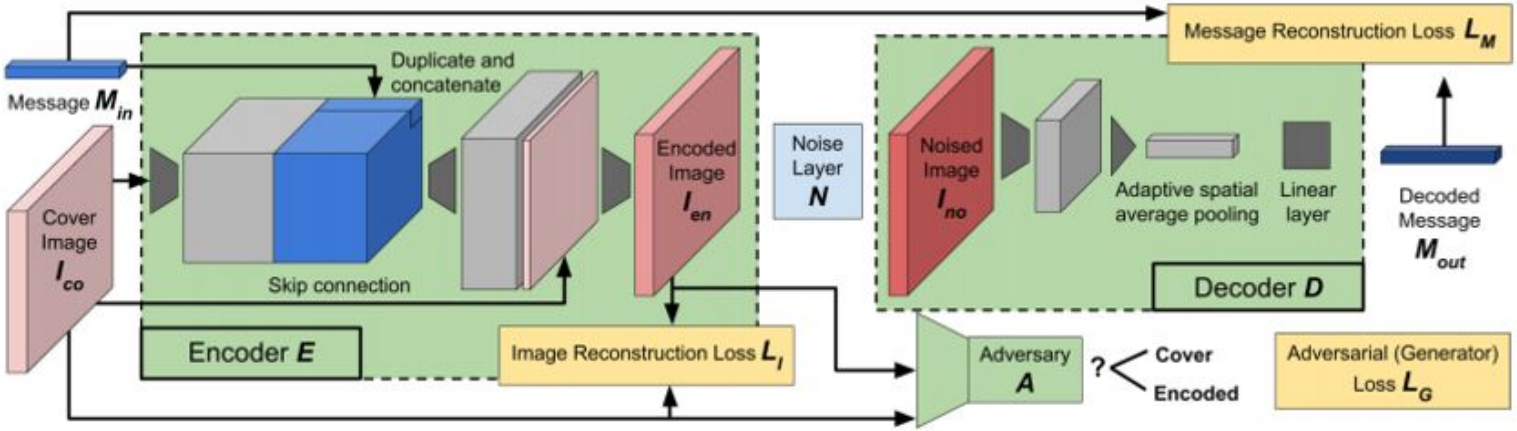


Fig. 1. Given a cover image and a binary message, the HiDDeN encoder produces a visually indistinguishable *encoded image* that contains the message, which can be recovered with high accuracy by the decoder.

Steganography



The Model

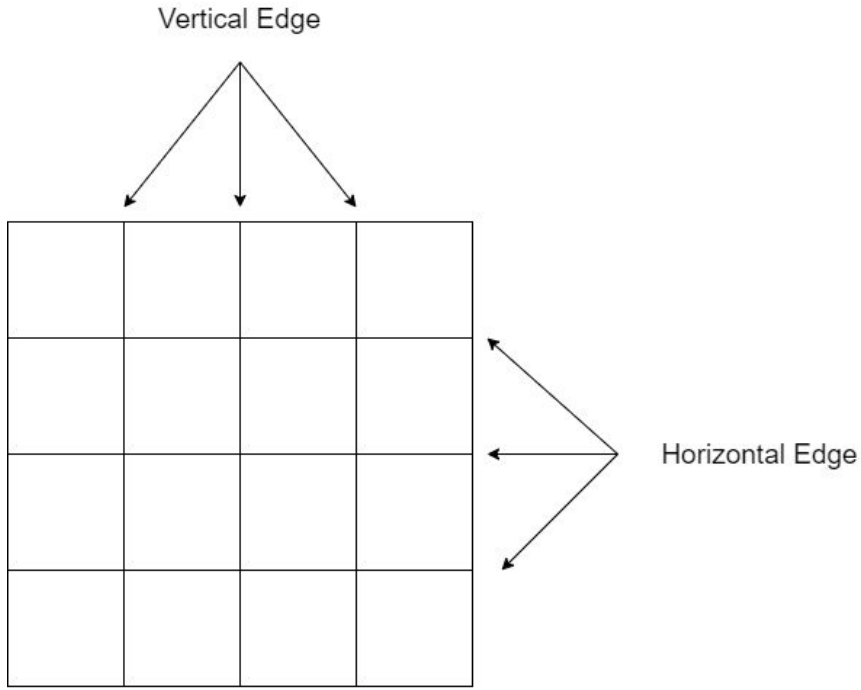

Message Reconstruction Loss L_M
Message M_{in}
Duplicate and concatenate
Cover Image I_{co}
Skip connection
Encoded Image I_{en}
Noise Layer N
Noised Image I_{no}
Adaptive spatial average pooling
Linear layer
Decoded Message M_{out}
Decoder D
Encoder E
Image Reconstruction Loss L_I
Adversary A
?
Cover
Encoded
Adversarial (Generator) Loss L_G

Divided block images.

Images might be divided into block, causing blocking effect that makes image looks not natural compared to the original images. We need to find a new metrics to reduce the blocking effect.

The “edge” is defined as distinct gray value between 2 pixel that makes it has an edged looks. So we propose a new loss, which count the number of pair in the horizontal and vertical edge on the total number of edged pairs.

$$EdgeLoss = (Hcount + Vcount)/Total$$



Text